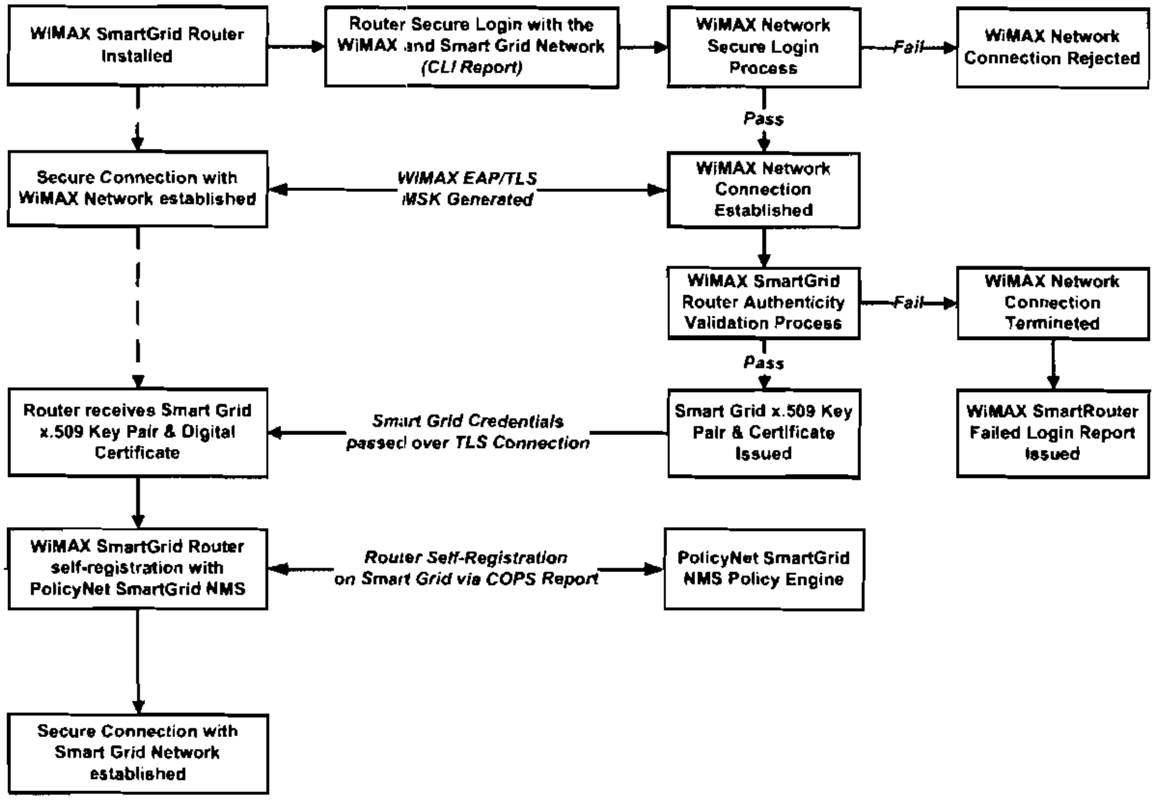

WiMAX SmartGrid Router Installed
Router Secure Login with the WiMAX and Smart Grid Network (CLI Report)
WiMAX Network Secure Login Process
Fail
WiMAX Network Connection Rejected
Pass
Secure Connection with WiMAX Network established
WiMAX EAP/TLS MSK Generated
WiMAX Network Connection Established
WiMAX SmartGrid Router Authenticity Validation Process
Fail
WiMAX Network Connection Terminated
Pass
Router receives Smart Grid x.509 Key Pair & Digital Certificate
Smart Grid Credentials passed over TLS Connection
Smart Grid x.509 Key Pair & Certificate Issued
WiMAX SmartRouter Failed Login Report Issued
WiMAX SmartGrid Router self-registration with PolicyNet SmartGrid NMS
Router Self-Registration on Smart Grid via COPS Report
PolicyNet SmartGrid NMS Policy Engine
Secure Connection with Smart Grid Network established

Figure 5 – Secure SmartGrid Network Entry Process by WiMAX SmartGrid Router by GE

Home Area Network Security

Secure HAN Communications functionality based on the IEEE 802.1.x (EAPOL) methods, which use EAP/TLS (or EAP/TTLS) to mutually authenticate a "utility registered" HAN device with the PolicyNet SmartGrid HAN Agent resident on the GE WiMAX SmartMeter over the meter's HomePlug HAN interface, will be available in the WiMAX Smart Grid Solution in the Fall of 2009. This HAN Device and GE WiMAX SmartMeter mutual authentication process (EAP/TLS or TTLS over RADIUS/IPSEC) utilizes the Meter's PolicyNet RADIUS Client and the PolicyNet HAN AAA (RADIUS) Server, which is located in a "non-routable quarantined" subnet on the Smart Grid Network.

As part of the PolicyNet software development process, Grid Net will be releasing an "open source" SmartGrid HAN SDK to the open source community. This SDK will contain the source code for an EAP/TLS (or TTLS) based Security Supplicant, a HAN SmartGrid WSDL based on the IEC CIM 61968-9 HAN extensions (currently being defined and developed by the US-based UtilityAMI working groups) and associated Java/XML and C/XML APIs.

It is both GE's and Grid Net's belief that this type of "open source" approach will foster the broad adoption of open standards-based, proven, broadly adopted methods, protocols, and algorithms for mutually authenticated, secure communications between "utility registered" HAN Devices and the PolicyNet SmartGrid HAN Agent on the GE WiMAX SmartMeter.

It is important to note that the meter's PolicyNet HAN Agent provides a layer 2 level secure, non-routable HAN Service Proxy Interface on the GE WiMAX SmartMeter over which both private and public HAN Messages and Signals can be exchanged with authorized service consumers. This HAN Service Proxy Interface prevents indiscriminate routing of packets onto the SmartGrid network, which lowers the risk profile of SmartGrid devices.

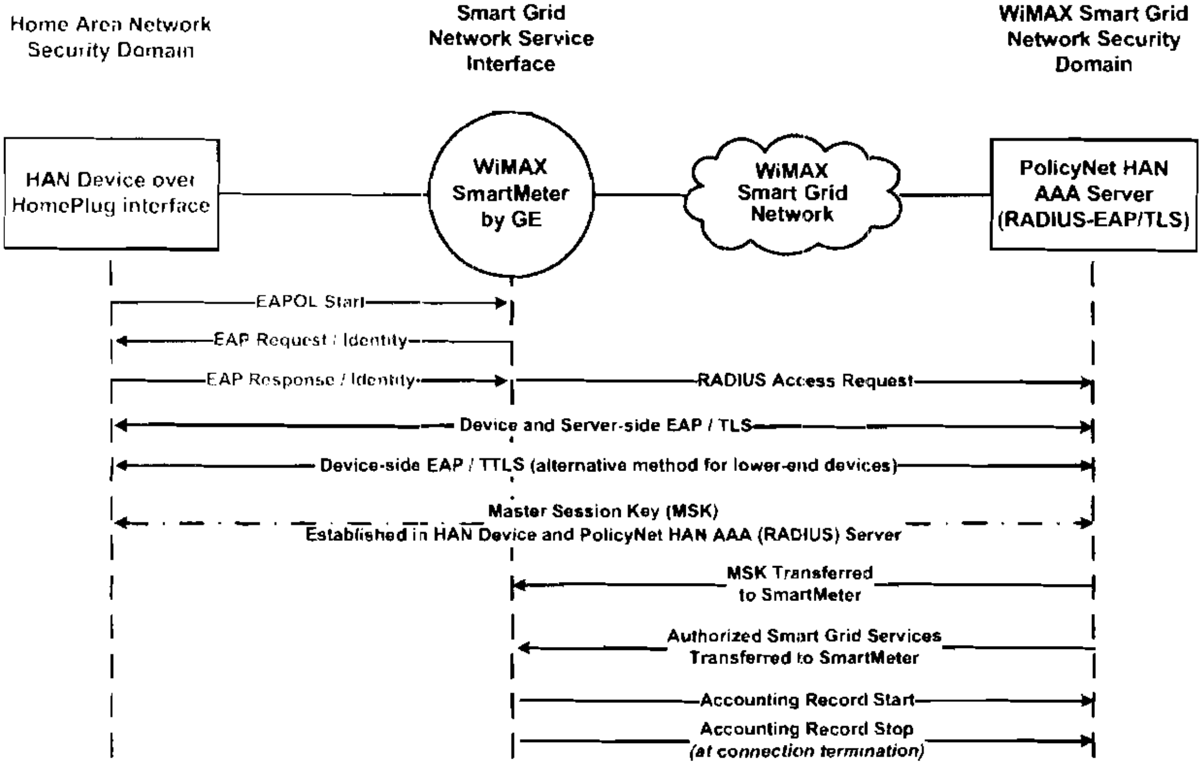

Home Area Network Security Domain
Smart Grid Network Service Interface
WiMAX Smart Grid Network Security Domain
HAN Device over HomePlug interface
WiMAX SmartMeter by GE
WiMAX Smart Grid Network
PolicyNet HAN AAA Server (RADIUS-EAP/TLS)
EAPOL Start
EAP Request / Identity
EAP Response / Identity
RADIUS Access Request
Device and Server-side EAP / TLS
Device-side EAP / TTLS (alternative method for lower-end devices)
Master Session Key (MSK)
Established in HAN Device and PolicyNet HAN AAA (RADIUS) Server
MSK Transferred to SmartMeter
Authorized Smart Grid Services Transferred to SmartMeter
Accounting Record Start
Accounting Record Stop (at connection termination)

Figure 6 – Secure SmartGrid Network Access Process by pre-registered HAN Device

WiMAX Security

As a full-featured telecommunication network infrastructure, WiMAX implements the highest commercial-grade, US Government certified, end-to-end security subsystem, including mutual device-to-device, device-to-system, and user-application authentication, service authorization, and billing-grade accounting, in order to support telecom-grade transaction levels – from delivery of traffic at various levels of service quality, e-commerce, new service deployment, and advanced content delivery mechanisms. Moreover, WiMAX is supported by the 500 member organizations (and engineering contributions) of the WiMAX Forum, which drive a vibrant ecosystem of rapid, cost-effective, standards-based innovations. No collector- or mesh-based

SmartGrid system has this level, depth or breadth of standards-based security support. The WiMAX Smart Grid solution takes full advantage of WiMAX's state-of the art security to deliver these security capabilities to Smart Grid networks. As described above, the WiMAX SmartMeter uses inherent WiMAX security provisions during various stages of the lifecycle. It is provisioned with a unique pair of WiMAX Forum Certified x.509 Certificates, and it receives a unique "digital signature" that is created by using the Crypto EEPROM chipset on the board and the AES-CMAC hashing algorithm that is used post mutual authentication to verify the "authenticity" of the meter. The IEEE 802.16.e PKMv2 protocol suite is used to securely bind the meter with the WiMAX base station.

WiMAX Smart Grid Network Security Domain

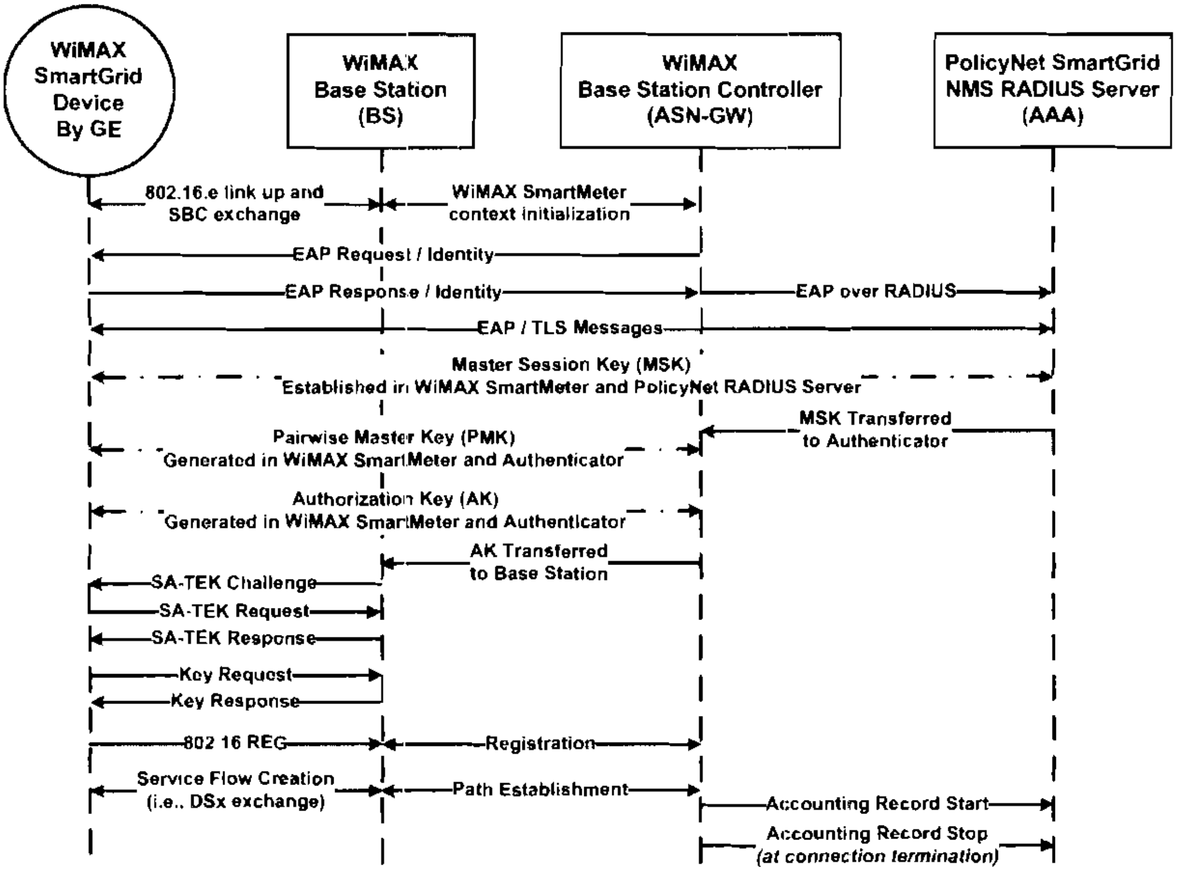

WiMAX SmartGrid Device By GE
WiMAX Base Station (BS)
WiMAX Base Station Controller (ASN-GW)
PolicyNet SmartGrid NMS RADIUS Server (AAA)
802.16.e link up and SBC exchange
WiMAX SmartMeter context initialization
EAP Request / Identity
EAP Response / Identity
EAP over RADIUS
EAP / TLS Messages
Master Session Key (MSK) Established in WiMAX SmartMeter and PolicyNet RADIUS Server
MSK Transferred to Authenticator
Pairwise Master Key (PMK) Generated in WiMAX SmartMeter and Authenticator
Authorization Key (AK) Generated in WiMAX SmartMeter and Authenticator
AK Transferred to Base Station
SA-TEK Challenge
SA-TEK Request
SA-TEK Response
Key Request
Key Response
802 16 REG
Registration
Service Flow Creation (i.e., DSx exchange)
Path Establishment
Accounting Record Start
Accounting Record Stop (at connection termination)

Figure 7 –WiMAX PKMv2-EAP/TLS Secure Network Access by SmartGrid Device by GE

PolicyNet SmartGrid NMS™ Security Components

COPS Security

COPS (Common Open Policy Service) and COPS-PR (COPS Usage for Policy Provisioning) are robust, versatile query / response protocol used in Grid Net's PolicyNet SmartGrid NMS software to exchange policy information between a Policy Decision Point (e.g., a PolicyNet server) and its Policy Enforcement Points (e.g., a SmartMeter endowed with a PolicyNet agent). Created for the general administration, configuration, and enforcement of policies in the telecommunications industry, COPS and COPS-PR are designed to be simple yet extensible, so that new kinds of Policy Enforcement Points (e.g., T&D devices) may be supported in the future without changing the protocol. The IETF RFC 2748 and RFC 3084 are international standards that cover the COPS and COPS-PR protocols. COPS provides strong message-level security for authentication, replay protection, and message integrity. COPS can also run over existing Internet security protocols such as IPSec or TLS.

Each Smart Grid device/user is a PEP (Policy Enforcement Point) Client and is authenticated via its SmartGrid Certificate when running COPS application traffic over the TLS protocol. The Authenticated PEP client is provided with a PEP ID, which is used as the Authorization Token. The following transactions take place:

1. The PDP (Policy Decision Point), in this case the PolicyNet server opens a COPS-PR/TLS Socket.

2. PEP sends its logical authentication, which presents Identity, Capability and Configuration over COPS/TLS.

3. PDP evaluates the PEP's logical authentication to determine appropriate policy provisioning for the PEP. The appropriate policies are then set over COPS-PR/TLS.

After the GE WiMAX SmartMeter gains secure network access to the Smart Grid Network, the PolicyNet SmartMeter Agent on the meter self-registers with the PolicyNet Policy Server utilizing the IETF COPS-PR/TLS protocol methods. During this self-registration process, a GE WiMAX SmartMeter Object is dynamically instantiated within the PolicyNet Policy Server's "in-memory database" where it registers its physical (hardware), logical (firmware), and operational (meter program and policies) properties. During this self-registration process, if there are any pending policy deployments for the meter (e.g., firmware upgrade policy, meter read policy, etc), then these policies are deployed to and enforced on the meter. After self-registration, the meter goes into "Disconnected COPS Mode", where the COPS-PR/TLS connection is released between the PolicyNet Policy Server and the Meter.

If a meter becomes de-energized, then its Smart Grid x.509 Digital Certificate and private/public key pair are deleted and revoked during the de-energized shutdown process. Upon power restoration, the meter must undergo the entire mutual authentication and authenticity validation processes to establish a secure network connection with the Smart Grid network.

All communications with the meter over its optical port require password based authentication and authorized access to the meter's C12.19 Data Table application (meter data recorder).

Database Security

PolicyNet is built on Oracle 11g -- database software that is known for employing the most advanced security methods and protocols currently available. However, PolicyNet further augments Oracle database security, as follows:

- The PolicyNet database schema implements a definer rights security model that limits access to data through an API implemented in Oracle PL/SQL. The only user authorized to connect to PolicyNet Database is the Policy Server. The Policy Server user only has permission to connect to the Database. In addition, the schema stores the binaries & certificates in SHA1 encrypted format.

- Database security is further enhanced by implementing application context security in addition to the definer rights security. The key security feature of application contexts is that they can only be written to by trusted functions that must be declared only when the context is created. Each user security context is checked by **sessionId** at the database and may only execute defined procedures. This is designed to prevent another client from connecting to the database with stolen Policy Server credentials and performing random operations (e.g., drop table, etc.).

It should be noted that this database security regime does not assume (or rely on) any features or behavior of applications outside of the database. Hence, the same level of security is enforced for any third-party application that can potentially be used to access the PolicyNet schema as the PolicyNet application itself.

Authentication and Authorization

For end-to-end authentication, the PKMv2-EAP (Extensible Authentication Protocol) methodology is used which relies on the TLS standard of public key encryption. EAP (EAP-TLS) is the framework used for authentication between the device (SmartMeter or SmartGrid Router) and the PolicyNet SmartGrid AAA RADIUS server (EAP/TLS-RADIUS) over the WiMAX network. The PKMv2-EAP protocol checks the X.509 certificate to authenticate the device. Data privacy is ensured by encrypting the data using Counter Mode with the Cipher Block Chaining Message Authentication Code Protocol (CCMP), which uses AES for transmission security and data integrity authentication.

Each user or system object that interacts with PolicyNet is managed internally with a set of associated roles and permissions for that user or system. Before any PolicyNet service can be invoked, the caller must authenticate by invoking Policy Server's Login() service to load the security context for that user or system. The Login() response contains a sessionId which the user or system must present in the SOAP header of every subsequent service invocation, similar to the way Kerberos service tickets are used as security tokens.

Upon login, a set of authorizations for that user or system is retrieved from the PolicyNet database, and this security context is loaded into both the Database and Policy Server memory for that session. Every service invocation checks the sessionId against an authorization map for that user or system before serving the request, both at the web-services layer and again at the data tier.

All communications between PolicyNet and the utility's enterprise systems (for example, such as those mentioned above), are established and maintained at the utility's discretion, via authorized PolicyNet web services and SOAP clients. Note that PolicyNet Web Services incorporate industry-standard, secure interfaces that enable utilities to securely and reliably incorporate essential functionality (as Smart Grid services) from enterprise systems into AMI systems. The PolicyNet web services API contains a broad array of standards-based interfaces (WS-I Basic Profile 1.0a compliant SOAP toolkits should correctly interoperate with PolicyNet web services and clients) based on the IEC Common Information Model (CIM) and the IEC 61968 Part 9 standards for Meter Reading and Control. CIM Compliance in this context is defined as follows:

- Compatibility with CIM classes, attributes, associations in data model implementation
- Message payloads based on a particular CIM version

To ensure secure communication between PolicyNet and other internal enterprise systems, all clients are required to authenticate with PolicyNet prior to invoking services. The authentication process loads a security context (set of permissions) in both the data tier and web services tier and returns a sessionId to authorized clients. A valid sessionId is passed as a security token with each service invocation. The web service tier and data tier both verify the permission set of the corresponding sessionId prior to serving requests. Session management is combined with transport security to reduce the threat of session high-jacking.

Future software releases will support SAML (Security Assertion Markup Language), developed by OASIS, which can be used for authentication and authorization against an Identity Provider via SOAP. SAML has three types of assertions: authentication, attributes, and authorization. The Service Provider provides an optionally signed assertion that always contains a timestamp, assertion ID, subject of the assertion (typically the user), and can also contain conditional information (e.g., time assertion remains valid).

Secure communications between the specified AMI system and third-party domains would be established and maintained at the discretion of BG&E. The method of secure communications for third-party applications and PolicyNet is the same as with PolicyNet and Internal-Enterprise Domain applications: PolicyNet – via its Web Services – can be configured to secure SOAP messages via TLS. The PolicyNet WSDL API contains a broad array of standards-based interfaces (WS-I Basic Profile 1.0a compliant SOAP toolkits should interoperate with PolicyNet web services) based on the IEC Common Information Model (CIM) and the IEC 61968 Part 9 standards Meter Reading and Control. CIM Compliance in this context is defined as follows:

- Compatibility with CIM classes, attributes, associations in data model implementation
- Message payloads based on a particular CIM version

Session Management

PolicyNet employs various measures against the threat of session hi-jacking:

- SOAP services run over TLS
- Each sessionId expires after a configurable period of time
- PolicyNet can be configured to refresh the sessionId with each request

Integrity

Data integrity is maintained at rest and in transit via industry standard protocols (TLS, IPSec) in a secure database to prevent unauthorized or undetected modification of the data. Input validation is performed on all input data to reduce the risk of attacks such as buffer overflows and SQL injection. Validation is performed at the web-services layer and again at the database.

The WiMAX SmartMeter supports 3 password privilege levels.

- **Customer Password** – has Read only privilege. This user password provides "READ Only" access to the meter's ANSI C12.19 Meter Data Recorder application
- **Reader Password** – Read and limited write (including time change) privilege. The "Reader Password" provides "READ/Limited WRITE" access and allows reading and setting the time.
- **Master Password** – Full Read/Write privilege. Master Password provides full READ/WRITE access.

PolicyNet will have Meter Password Management capability which will enable all meters to have a unique set of ANSI C12.19 Data Table Application User ID/Passwords. In addition, this functionality will use randomly generated passwords, which are changed periodically based on "password aging rules" that are defined by the PolicyNet SmartGrid NMS Administrator account(s).

Auditing / Logging – Record Program Access & Changes

The meter's security log includes:

SECURITY LOG

Number of Bad Passwords	All
Number of Demand Resets	All
Number of EEPROM Writes	All
Number of OPTOCOM Communications	All
Number of Power Outages	All
Number of Times Programmed	All
Number of Times for Real-Time Pricing Entries	All
Cumulative Power Outage Duration in seconds	TOU/DmdLP
Date of Last Calibration	All
Time of Last Calibration	All
Date of Last Demand Reset	TOU
Time of Last Demand Reset	TOU
Date of Last OPTOCOM Comm.	TOU
Time of Last OPTOCOM Comm.	TOU
Date of Last Power Outage	TOU/ DmdLP
Time of Last Power Outage	TOU/DmdLP
Date of Last Programming	All
Time of Last Programming	All
Date of Last Real-Time Pricing Entry	TOU
Time of Last Real-Time Pricing Entry	TOU
Date of Last Time Change	TOU
Time of Last Time Change	TOU

In addition, PolicyNet logs all user operations including data inserts/updates/deletes and policy deployments, using the User Id presented to the **Login** service and a timestamp to provide a complete Audit Trail which may be viewed by authorized users invoking the **searchAuditTrail** service. Attempted database operations from clients outside the server are also logged. The sessionIds and user passwords are one-way hash encrypted to provide acceptable risk against collision by an attacker.

Newington Smart Community Trial

HAN Requirements

Document History

Revision History

Version	Rev. Date	Summary of Changes	Author

Approvals

Name	Title / Responsibility	Signature	Date

Reviewers

Name	Area of Expertise

Distribution

Name		

Table of Contents

1 Introduction

This document provides details of EA's requirements of HAN Vendors as part of the solution component for the Newington Smart Community Trial project.

1.1 Purpose

The purpose of this document is to define the HAN requirements to be forwarded to HAN Vendors to ensure the conceptual design of the trial solution is feasible. The document allows short listed vendors from the EA Newington HAN Vendor FRI process to take the next step in the selection process to indicate to EA the level of capability and compliance (or intention of compliance) to Open HAN standards of their proposed solution.

1.2 Abbreviations

Term	Description
AMI	Automated Metering Infrastructure
BOM	Bureau of Meteorology
DC	Distribution Centre
DB	Database
DM&C	Distribution Monitoring & Control
DRED	Demand Response Enabling Device
HAN	Home Area Network
HV	High Voltage
IHD	In Home Display
LV	Low Voltage
MDI	Maximum Demand Indicator
MMS	Meter Management System
MV	Medium Voltage
Newington	Newington Smart Community Trial
PINC	Platform for Intelligent Network Communications
PQ	Power Quality
PSS/E	Power Systems Simulator for Engineering
PV	Photovoltaics
TCA	Testing Certification Australia
TOU	Time of Usage

2 HAN Requirements

The EA Newington Smart Community Trial includes the deployment of 1000 smart meters with differing levels of energy usage information and control being provided to subsets of those customers. In addition there will be at least 500 water meters able to provide at least daily water consumption data. The key objective is to understand the incremental impact that each "tool" may have on customer energy and water usage. Those tools include:

- 100 Home Area Networks (HAN) with individual appliance energy metering and on/off control. The HAN display will be via a web portal that is accessible locally or remotely. It will display real time data in 5 minute intervals, with historical comparisons, and include water data;
- 100 In Home Devices (IHD) that will provide gross real time household energy consumption data and historical usage.
- The balance of the homes are likely to have access to a Web Portal that provides gross energy usage and water data. In addition the portal will be used as the basis for developing a community engagement with the project, by offering education and incentives on energy and water usage.

The implementation of the HAN is likely to require the following hardware components per home:

- 5 x appliance sub meters that are both able to measure total energy usage and provide basic on/off functionality to that device via the HAN interface. These devices are likely to be installed with appliances such as TV, fridge, clother dryer, washing machine etc. Therefore these sub meters need to be rated for 10A; should the load be a significant inductive device (eg. a motor), the sub meter should be rated up to 15A.

- 3 x hardwired CT module with pulse output, that provides the same functionality as the above sub meter, but can be used for such appliances as the lighting circuit, hot water system and air conditioner. The pulse output would also need to interface with the meter/HAN controller. These modules must be rated to 63A. Future requirements may include 3 phase monitoring on consumer circuits.

- 1 x HAN controller to collect the information from each of the sub meter modules, including the hardwired CTs.

- 1 x Temperate sensor that provides near real time internal temperate to the HAN controller

The Newington customer has access to information on device energy consumption from HAN in 2 ways:

- directly via HAN Controller terminal
- via a Customer Portal

The diagram below represents the conceptual architecture for the Newington trial and represent key requirements.

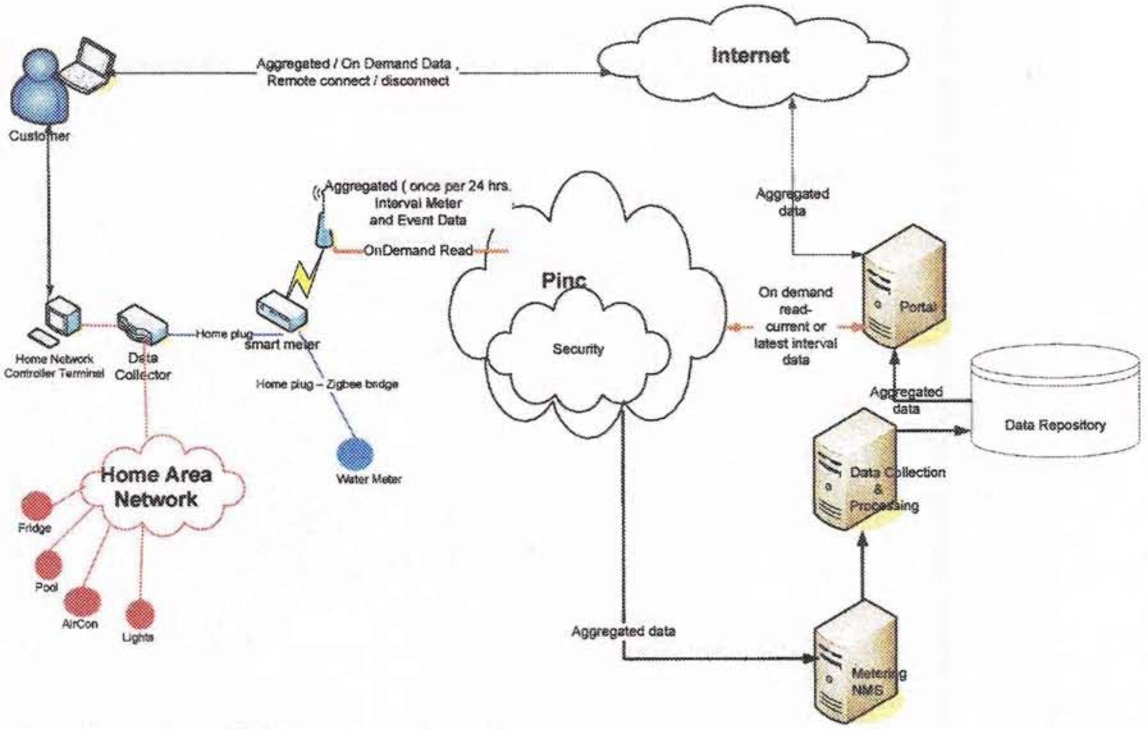
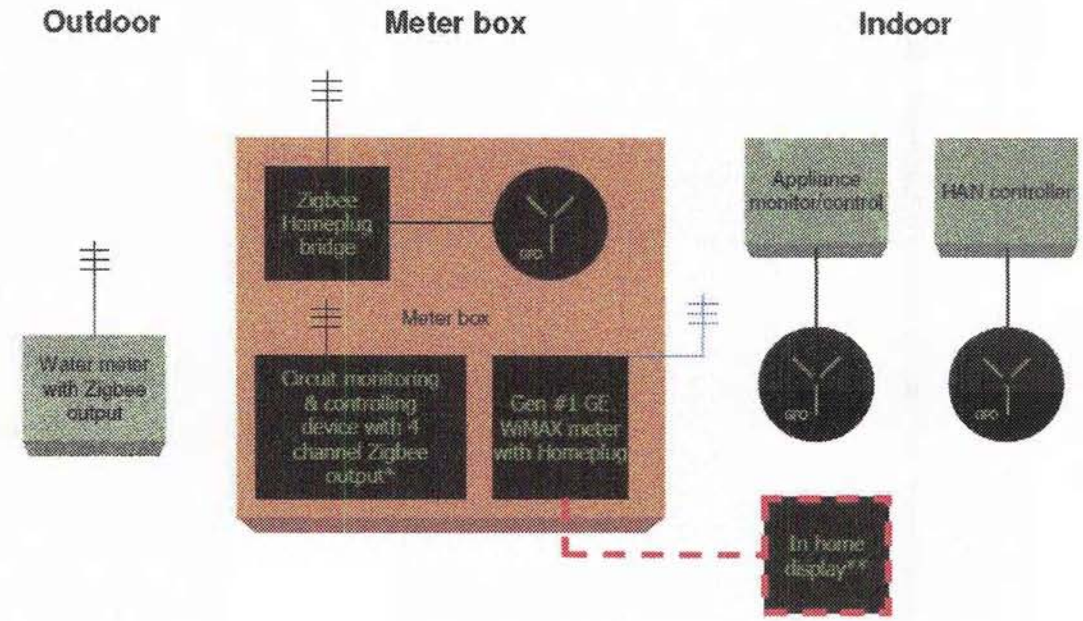

Aggregated / On Demand Data ,
Remote connect / disconnect
Internet
Customer
Aggregated (once per 24 hrs. Interval Meter and Event Data
OnDemand Read
Pinc
Security
Aggregated data
On demand read- current or latest interval data
Portal
Aggregated data
Data Repository
Data Collection & Processing
Home Network Controller Terminal
Data Collector
Home plug
smart meter
Home plug – Zigbee bridge
Water Meter
Home Area Network
Fridge
Pool
AirCon
Lights
Aggregated data
Metering NMS

Figure 1 : Conceptual HAN requirement overview


Outdoor
Meter box
Indoor
Zigbee Homeplug bridge
GPO
Meter box
Water meter with Zigbee output
Circuit monitoring & controlling device with 4 channel Zigbee output*
Gen #1 GE WiMAX meter with Homeplug
Appliance monitor/control
HAN controller
GPO
GPO
In home display**

*This assumes the Zigbee Homeplug bridge can support multiple connections; it may need pulse output to Zigbee conversion, and therefore power.
**IHD may interface with the meter using wired or wireless communications.
**IHD can exist independently of the HAN system.

Figure 2 : HAN Hardware Map

The key requirement for the HAN vendor to confirm is:

HAN API's exist that allow web service requests to retrieve appliance usage data in real time.

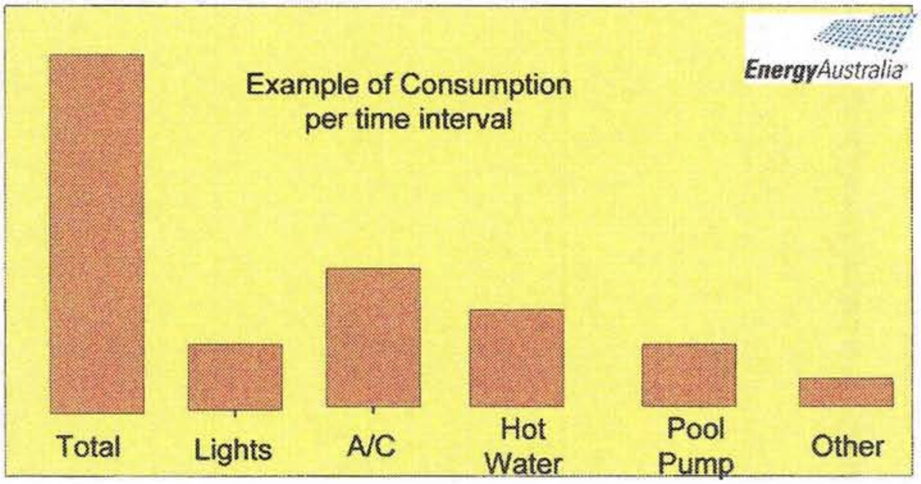
The 'customer portal' is a key component of the trial. The portal will primarily provide information to the customer of usage data.
The function of the portal will have two facets –

- Display consumtpion data that describes usage now. This data is sourced from the devices directly – the HAN (& the meter).
- Display consumption data that describes usage through time. This data is sourced from the metering data repository (collected regularly)

3 *High Level EA HAN Requirements*

The HAN capabilities need to support the following EA requirements & the vendor is expected to have published API's to support the requirements:

- Register individual appliances in HAN including appliances, Water meters, Distributed Generation and Storage devices .
- Collect consumption data for all registered appliances in the data collector and support forwarding that data to an NMS on a regular basis (daily).
- Communications to the meter using Home-plug or enable an appropriate bridge to Home-plug. For example; Zigbee / Home-plug bridging devices are commercially available.
- Supply and Display individual appliance current consumption information
- Supply and Display individual appliance aggregated consumption information for multiple consumption intervals ranging from one minute time intervals to days to months.
- A required portal consumption display is conceptually described in the diagram below – consumption at the meter with details of consumption for all HAN devices (plus 'other').



- Support requests to the NMS or Meter to display consumption at the meter
- Support HAN device control (turn on/off) locally
- Support HAN device control (turn on/off) remotely from web portal
- Support Security and authentication as per HAN specification
- Support broadcast notification messages
- Each of the requirements listed must be supported by published APIs using SOAP/XML such that HAN can integrate into both Portal and Meter.

4 HAN and Open Standards

Vendors should discuss their position with respect to open standards and related groups such as the following groups:

> http://osgug.ucaiug.org/utilityami/AMIENT/Meetings%20Agendas%20and%20Docs/
> Palo%20Alto%20-
> %20January%202009/HAN_SmartEnergyProfile_Dec2008.ppt#256,1,ZigBee® +
> HomePlug® Joint Working Group - The SmartEnergy Profile

EA is interested in partnering with vendors that intend to work in an Open Standards environment. As such the following HAN specifications have been provided to allow vendors to indicate the extent of their support-for and progress-towards the following Open HAN specification extract. For the purposes of EA & the Newington trial references to AMI Gateways would be the proposed Network Management System (NMS) being used by EA in the trial. Please provide compliance discussions to the following requirements from the Open HAN specification:

Category	Number	Requirement	EA Priority

Application: Control			M=Mandatory
			N=Nice to have
			F=Future

	1	HAN Device shall accept control signals from the Utility.	M
	2	HAN Device shall respond to requests to cease operational state (e.g., open contact).	M
	3	HAN Device shall respond to requests to resume operational state (e.g., close contact).	M
	4	HAN Device shall acknowledge receipt of control signal.	M
	5	HAN Device shall acknowledge execution of control request.	M
	6	HAN Device shall acknowledge execution failure of request (i.e., exceptions).	M
	7	HAN Device shall signal any consumer-initiated overrides.	M
	8	HAN Device shall respond to request to cease operation state at a specific time.	M
	9	HAN Device shall respond to request to resume operation state based at a specific time.	M
	10	HAN Device shall delay restoration of operational state based on a pre-configured time (e.g., random number).	M
	11	HAN Device shall respond to request to cycle operational state (i.e., duty cycle).	M
	12	HAN Device shall respond to request to limit operational state based on thresholds, set-points or triggers (e.g., price points).	M
	13	HAN Device shall respond to requests for variable output (e.g., load limiting, energy savings mode)	M

Application: Measurement			
	1	HAN Device shall measure instantaneous demand (e.g., W).	M
	2	HAN Device shall measure accumulated consumption (e.g., Wh).	M
	3	HAN Device shall measure accumulated production (e.g., Wh).	M
	4	HAN Device shall measure consumption per interval (e.g., Wh, BTU, HCF).	M
	5	HAN Device shall measure production per interval (e.g., Wh).	M
	6	HAN Device shall store intervals measurements (e.g., 30 days of interval reads).	M
	7	HAN Device shall allow interval configuration (e.g., 15 Minutes).	M
	8	HAN Device shall monitor energy state (e.g., state of charge).	M
	9	HAN Device shall measure available capacity (e.g., W, Volt-Amps).	M
	10	HAN Device shall monitor the operational mode (e.g., charging, discharging).	M
	11	HAN Device shall measure power quality (e.g., frequency, neutral voltage, harmonic content).	M
	12	HAN Device shall monitor environmental state (e.g., temperature, motion, wind).	M
	13	HAN Device shall monitor the operational mode of other devices (e.g., duty cycle).	M
	14	HAN Device shall monitor environmental impact (e.g., CO2).	N
Application: HAN UI			
	1	HAN Device shall provide visual indicators which indicate operational state (e.g., commissioned, registered, event status, device state).	M
	2	HAN Device shall provide a power cycle input, which reboots the device.	M
	3	HAN Device shall provide a user reset input, which returns the device to its pre-installation state (e.g., button).	M
	4	HAN Device shall provide an alphanumeric display which indicates operational state (e.g., LCD screen).	M
	5	HAN Device shall provide non-visual sensory feedback (e.g., motion, vibration, audible).	N
	6	HAN Device shall provide a sight and hearing impaired interface.	N
	7	HAN Device shall provide a user-configurable display.	M
	8	HAN Device shall accept user configurations.	M

	9	HAN Device shall accept user preferences (e.g., Celsius/Fahrenheit, color).	N
	10	HAN Device shall provide alarm notifications (e.g., price threshold, event messages).	M
	11	HAN Device shall accept Utility data source configurations (e.g., AMI Gateway, other HAN Devices).	F
	12	HAN Device shall display Utility data source configurations (e.g., AMI Gateway, other HAN Devices).	F
	13	HAN Device shall display application-specific information (e.g., cost, consumption, environmental impact, payment credit, remaining account credit).	F
	14	HAN Device shall accept application-specific configurations (e.g., preconfigured periods (e.g., hour, day, week), configurable periods (e.g., interval length, TOU period), variable periods (e.g., Critical Peak Price period).	F
	15	For battery-powered devices, HAN Device shall provide a battery life indicator.	M
	16	HAN Device shall accept payment data from the consumer.	F
Application: Processing			
	1	The application shall calculate a HAN Device's estimated energy cost of accumulated energy consumption as monetary value (e.g., $/kWh * accumulated kWhrs = $).	N
	2	The application shall calculate a HAN Device's estimated energy cost of instantaneous power consumption as a monetary value per time interval, (e.g., $/Wh * instantaneous W= $/hr).	N
	3	The application shall calculate a HAN Device's estimated cost for Hourly Energy rates.	N
	4	The application shall calculate a HAN Device's estimated energy cost for rate tiers/energy blocks.	N
	5	The application shall calculate a HAN Device's estimated energy cost for Time-of-Use (TOU) energy rates.	N
	6	The application shall calculate a HAN Device's estimated cost for Critical Peak Pricing (CPP).	N
	7	The application shall calculate a HAN Device's estimated cost for capacity billing rates.	N
	8	The application shall calculate estimated costs for other billing determinants (e.g, monthly customer charges, taxes & franchise fee, surcharges, discounts, ratcheted demand, bond charges).	F
	9	The application shall accept aggregated consumption and rate information from user-configurable sources (e.g., AMI Gateway, AMI System, and/or HMI).	F
	10	The application shall calculate and forecast a HAN	F

		Device's consumption based on user-defined parameters (e.g., estimated kWh/mon).	
	11	The application shall calculate and forecast a HAN Device's production based on user-defined parameters (e.g., estimated kWh/mon).	F
	12	The application shall forecast a HAN Device's estimated cost calculation based on user-defined parameters (e.g.	F
	13	The application shall calculate a HAN Device's consumption based on user-defined parameters (e.g.	F
	14	The application shall calculate a HAN Device's production based on user-defined parameters (e.g.	F
	15	The application shall calculate and/or predict a HAN Device's environmental impact based on user-defined parameters (e.g.	F
	16	The application shall supply a method for local billing resolution (e.g.	F
	17	The application shall calculate and suggest methods to optimize energy consumption and cost based on user-defined parameters (e.g.	F
	18	The application shall calculate a HAN Device's relative efficiency (e.g.	F
	19	The application shall calculate available load for demand reduction based on user-defined parameters (e.g.	N
	20	The application shall calculate user-defined thresholds for consumption	N
Communications: Commissioning			
	1	HAN Device shall accept network configuration data which allows for private Utility networking (e.g., private address/ID)	M
	2	HAN Device shall accept commissioning configuration data by the manufacturer (e.g., link key).	M
	3	HAN Device shall accept commissioning configuration from the Installer.	M
	4	When a **HAN Device** is triggered (e.g., Allow Join Command), HAN Device location-specific/contact-specific data shall be provided to other HAN Devices in the premise.	M
	5	When a HAN Device is triggered (e.g. Power-on, button), HAN Device shall provide the AMI Gateway with device specific information including device ID and device type.	M
	6	When a HAN Device is triggered (e.g. power on, button), HAN Device shall provide the AMI Gateway with device specific Utility information, including network ID, gateway ID, and Utility ID, if pre-configured with Utility information.	M
	7	**HAN Device** shall have the ability to accept or reject the request based on device type.	M

	8	**HAN Device** shall have the ability to accept or reject device requests based on Utility specific information, including network ID, gateway ID, and Utility ID.	M
	9	**HAN Device** shall acknowledge successful commissioning requests (i.e., provide acknowledgement to the requesting HAN Device).	M
	10	When a HAN Device is communicating with the AMI Gateway, HAN Device shall indicate link connectivity.	M
	11	HAN Device shall provide notification to the Installer of the commissioning status. Status conveyed shall be either: successful/unsuccessful.	M
	12	**HAN Device** shall maintain an updated list of commissioned (i.e., connected) HAN Devices.	M
	13	**HAN Device** shall have the ability to remove HAN Devices from the Utility HAN.	M
Communications: Control			
	1	HAN Device shall accept network organization messages from the AMI Gateway (e.g., gateway location, routing table, address).	M
	2	HAN Device shall accept network organization messages from peer devices (e.g., hidden node).	M
	3	HAN Device shall use the most reliable path to the AMI Gateway (e.g., based on signal strength/quality).	M
	4	HAN Device shall only use routes within its logical network (e.g., network ID, address scope, Utility ID).	M
	5	HAN Device shall support prioritization of traffic (e.g., queuing, scheduling, traffic shaping).	M
	6	HAN Device shall have the ability to automatically adapt to communications interference through detection and analysis of environmental conditions (e.g., channel hopping, channel avoidance, signal-to-noise ratio).	M
	7	HAN Device shall have the ability to automatically adapt to range constraints through detection and analysis of environmental conditions (e.g., change modulation schemes, change power output levels).	M
	8	HAN Device shall include a data integrity mechanism for all communications.	M
	9	**HAN Device** shall have the ability to activate and deactivate its HAN communication.	M
	10	HAN Device shall communicate its availability (i.e., 'heartbeat') to the AMI Gateway at least once per day.	M
	11	HAN Device shall have a configurable availability communication (i.e., heartbeat) frequency to the AMI Gateway.	M
	12	**HAN Device** shall store a list of available HAN Devices in the premise and make that list available to the AMI System upon request.	M
Security: Access			

	1	**HAN Device** shall provide access control to Utility applications, data, and services (e.g., control data, consumer-specific consumption data).	M
	2	HAN Device shall control access to persistent Utility HAN data (data at rest).	M
	3	HAN Device shall control access to transmitted Utility HAN data (data in transit).	M
	4	**HAN Device** shall provide protection of Utility HAN data while being processed (data in processing) (e.g., trusted processor).	M
	5	**HAN Device** shall control access to data in accordance with a configurable Utility security policy (e.g., users, applications, devices, data access-read/write).	M
	6	**HAN Device** shall provide mechanisms to enforce a policy based on least privilege (i.e., explicit authorization).	M
	7	**HAN Device** shall have the ability to enforce policy periods (time constraints) for security policy elements (e.g., maintenance/firmware window).	M
	8	HAN Device shall control access to data in accordance with a configurable Utility security policy (e.g., users, applications, devices).	M
	9	**HAN Device** shall provide methods to query and report access control data settings.	M
	10	HAN Device shall provide access control methods which prevent known attacks, including replay, man-in-the-middle, delay, spoofing, sequence change, and deletion attacks.	M
	11	HAN Device shall implement mechanisms to prevent unintended disclosure of source/originator data to unauthorized principals.	M
	12	HAN Device shall implement controls which limit access to audit information.	M
	13	HAN Device shall support confidentiality and access controls that employ cryptographic operations (e.g., digital signatures).	M
	14	HAN Device shall support confidentiality and access controls that employ cryptographic keys for only one purpose (e.g., encryption authentication, or digital signatures).	M
		HAN Device shall provide access control to Utility applications, data, and services (e.g., control data, consumer-specific consumption data).	M
Security: Integrity			
	1	HAN Device shall protect the integrity of the HAN system (e.g., shall not adversely impact the operations of the HAN system by introducing malicious or unintended activity).	M

	2	**HAN Device** shall provide a configurable HAN filtering function that filters based on allowable message types.	M
	3	**HAN Device** shall provide a configurable HAN filtering function that filters messages based on structural integrity of the message.	M
	4	**HAN Device** shall provide a configurable HAN filtering function that filters based on allowable message rates.	M
	5	HAN Device shall detect unauthorized modification of data during storage (e.g., check sums, hashes, software attestations).	M
	6	HAN Device shall detect unauthorized modification of data during network transit (e.g., check sums and hashes).	M
	7	HAN Device shall attempt to correct unauthorized modification of data (e.g., resend).	M
	8	HAN Device shall detect unauthorized modification of data attributes (e.g., modification to a message type).	M
	9	HAN Device shall attempt to correct unauthorized modification of data attributes.	M
	10	HAN Device shall only accept data from an authorized source (e.g., AMI Gateway, certified EMS).	M
	11	HAN Device shall protect the system from malicious code (e.g., buffer overflow protection, limit executable code exposure).	M
	12	HAN Device shall detect known attacks, including replay, man-in-the-middle, delay, spoofing, sequence change, and deletion attacks.	M
	13	HAN Device shall separate security critical functionality and data from non-security critical system data.	M
	14	**HAN Device** shall validate the source of HAN security policy.	M
	15	**HAN Device** shall detected unauthorized modification of HAN security policy.	M
	16	HAN Device shall detect unauthorized modification of audit data.	M
	17	HAN Device shall validate the integrity of all software updates, including source, structure, and version.	M
	18	HAN Device shall use tamper-resistant hardware (e.g., epoxy, TPM).	M
Security: Accountability			
	1	HAN Device shall alert the AMI Gateway of all detected, security –related activities, including access control, authentication, and integrity violations.	M
	2	HAN Device shall audit and store all security-related activities, including access control, authentication,	M

		registration, and integrity violations.	
	3	HAN Device shall provide, at a minimum, the following information for all detected security events: date and time of the event, type of event, device/user identity.	M
	4	HAN Device shall provide the AMI System access to audit data.	M
	5	**HAN Device** shall provide non-repudiation mechanisms for devices and users.	M
	6	**HAN Device** shall provide a mechanism for source identification of data (e.g., HAN and AMI System data).	M
	7	**HAN Device** shall provide the capability to audit both system and user operations as defined by the HAN security policy.	M
	8	HAN Device shall provide the ability to perform searches, sorts and filters of audit data based on date and time, type and/or user identity.	M
	9	HAN Device shall provide the capability to identify mandatory and configurable audit elements (In this context, mandatory refers to audit elements which are always enabled and configurable refers to audit elements which can be enabled or disabled at the discretion of the Consumer or Utility).	M
Security: Authentication (Registration)			
	1	HAN Device shall support mutual authentication.	M
	2	HAN Device shall authenticate the source of all control signals.	M
	3	HAN Device shall provide a mechanism which allows for multiple and configurable authentication materials (e.g., device ID, device type, key, serial key, utility ID, and device configuration).	M
	4	HAN Device shall be configured with utility-approved or -provided authentication materials (e.g., certificate, key).	M
	5	HAN Device shall not send authentication materials over the network in an insecure fashion (e.g., do not transmit passwords or keys in the clear).	M
	6	HAN Device shall be compatible with a utility-defined registration process.	M
	7	HAN Device shall provide a means to update (i.e., change, reconstitute, rollover) authentication materials.	M
	8	**HAN Device** shall allow registration revocation for connected HAN Devices.	M
	9	HAN Device shall support a configurable registration and expiration period (e.g., registration timeout, registration persistence).	M
	10	HAN Device shall use security services (i.e., cryptographic services) which are either FIPS-approved or	N

		NIST-recommended.	
	11	HAN Device shall support a registration method that employs cryptographic operations (e.g., digital signatures).	M
	12	**HAN Device** shall provide an authentication mechanism which proxies for the AMI System (e.g., negotiates on behalf of the utility).	M
	13	HAN Device shall provide notification to the Installer of the registration status. Status conveyed shall be either: registered/not registered	M
Performance			
	1	HAN Device shall supply functionality that maintains communications availability to the AMI Gateway.	M
	2	HAN Device shall supply functionality that maintains application availability to the AMI System (e.g., software/hardware application watchdog).	M
	3	After loss of power, HAN Device shall return to its post-configuration state (i.e., shall persist communication and registration configurations).	M
	4	HAN Device shall supply adequate computational performance (i.e., Device shall not hamper overall operational state of the HAN)	M
	5	HAN Device shall supply adequate communications performance (e.g., bandwidth and throughput).	M
	6	HAN Device shall supply accurate time keeping and counter functions.	M
	7	HAN Device shall not act on expired signals (e.g., message validity duration or sequence).	M
	8	HAN Device shall provide configurable communications such that system is scalable (e.g., heartbeat and request frequency).	M
	9	HAN Device with battery power shall function for a minimum of 1 year.	M
	10	HAN Device shall supply a local software upgrade function (i.e., firmware upgrade).	M
	11	HAN Device shall supply a remote software upgrade function (i.e., firmware upgrade).	M
	12	HAN Device shall meet the quality, interoperability, and testing (i.e., certification) requirements of its respective technology platform body.	M
Operations Maintenance & Logistics: Manufacturing			
	1	Prior to installation (e.g., factory, depot), a HAN Device shall support placement of commissioning data (e.g., pre-placed network key).	M
	2	Prior to installation (e.g., factory, depot), a HAN Device shall support placement of registration data (e.g., pre-	M

		placed registration key).	
	3	HAN device shall support pre-placed methods or materials that support commissioning and registration by multiple utilities (does not imply simultaneous Utility registration).	M
	4	HAN Device shall support pre-placement of application-specific configurations (e.g., cost, consumption, environmental impact, configurable time/rate intervals).	M
	5	HAN Device shall have and display appropriate certification (e.g., UL, ANSI, and FCC) on its packaging and body.	M
	6	HAN Device shall have and display appropriate commissioning and registration information on its packaging and body (e.g., serial number, registration code).	M
	7	HAN Device shall display Utility compatibility guidance to verify that a HAN Device is compatible with a particular AMI system.	M
	8	HAN Device shall display its HAN network technology compatibility on its outside packaging.	M
	9	HAN Device shall display UtilityAMI compliance.	M
	10	HAN Device shall display Enhanced UtilityAMI compliance.	M
	11	The HAN device shall display, on its packaging, any secondary device requirements (e.g., required EMS, bridge device).	M
	12	HAN Device shall be manufactured to support multiple distribution channels (e.g., retail, direct Utility).	M
Operations Maintenance & Logistics: Installation			
	1	HAN Device Manufacturer shall include installation documentation, which includes instructions for installation (e.g., placement), commissioning, and registration, including any external dependencies.	M
	2	HAN Device Manufacturer shall include a HAN Device user's manual in the Device packaging.	M
	3	HAN Device Manufacturer shall include Manufacturer contact information in the Device packaging.	M
	4	HAN Device Manufacturer shall supply technical support services (e.g., help desk, web site).	M
Operations Maintenance & Logistics: Maintenance			
	1	HAN Device shall have a self-check (initialization) function, which notifies the Installer that the HAN Device is functioning properly.	M
	2	**HAN Device** shall log all AMI System-to-HAN System	M

		communications.	
	3	When the HAN Device is rebooted, HAN device shall reset to its configured (i.e., post-installation commissioning and registration) state and shall reestablish communication with the AMI Gateway.	M
	4	HAN Device shall have a user-operable testing function that is equivalent to the self-testing function.	M
	5	HAN Device shall supply a maintenance port for field diagnostics.	M
	6	HAN Device shall simulate Utility events for diagnostic purposes.	M
	7	HAN Device shall supply network management functions for diagnostic purposes.	M
	8	For battery-powered devices, HAN Device shall communicate low battery state to the AMI System.	M
	9	HAN Device Manufacturer shall supply and support a flaw remediation process.	M
	10	HAN Device shall support a communications feedback mechanism (i.e., ping).	N